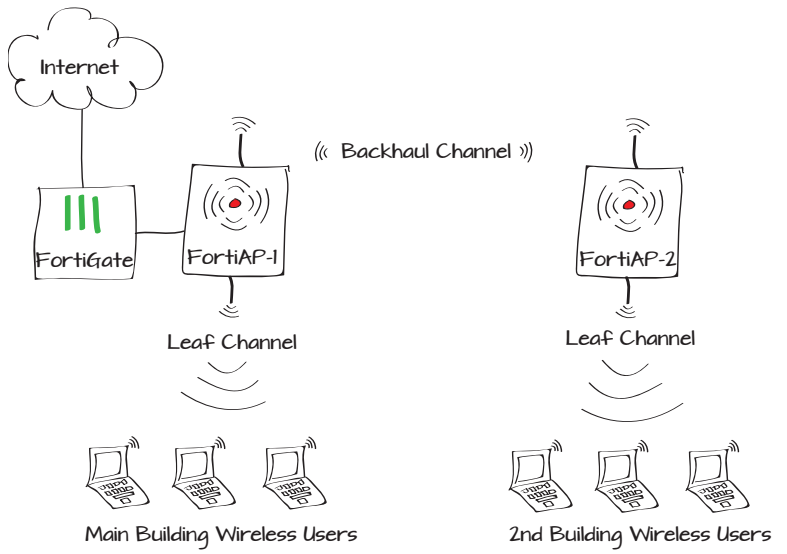
Extending the range of a wireless network by using mesh topology

This example demonstrates how to configure a FortiGate and two FortiAP wireless access point units to extend the reach and availability of a wireless network. This example simulates a company that has expanded into a second, nearby building that requires wireless access.

The FortiAP units used to create a wireless mesh must be models that have two radios.

1. Configuring an interface on the FortiGate for the APs
2. Creating two SSIDs
3. Creating a custom AP profile
4. Creating firewall addresses and an address group
5. Setting up and configuring the FortiAPs
6. Creating security policies on the FortiGate
7. Results



Before you begin

The following models were used in this example: FortiGate-100D, FortiAP-220B, and FortiAP-221B.

The FortiGate unit is in Interface Mode (each physical port can be the interface to a distinct subnet), so that a single port, in this case 11, will be used for the sole purpose of interface for the wireless network.

The computers managing the network and FortiAPs are located on the internal network.

Configuring an interface on the FortiGate for the APs

A dedicated network interface needs to be configured on the Fortigate that will be used only by the FortiAP units.

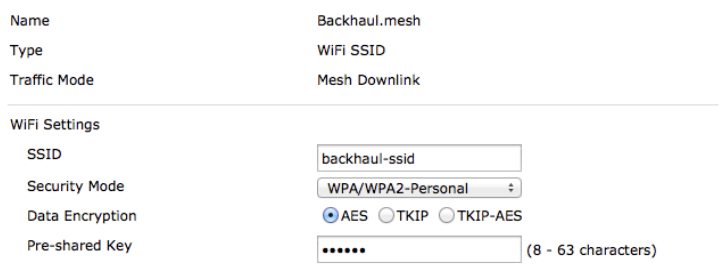
Go to **System > Network > Interfaces** and edit an available internal port (in the example, port11). Set **Addressing mode** to **Dedicate to FortiAP/FortiSwitch**.

Creating two SSIDs

A wireless mesh requires two SSIDs: back-haul and leaf. The backhaul channel is the wireless connection between the two FortiAP units, while the leaf channel is used by individual clients to connect to the wireless network.

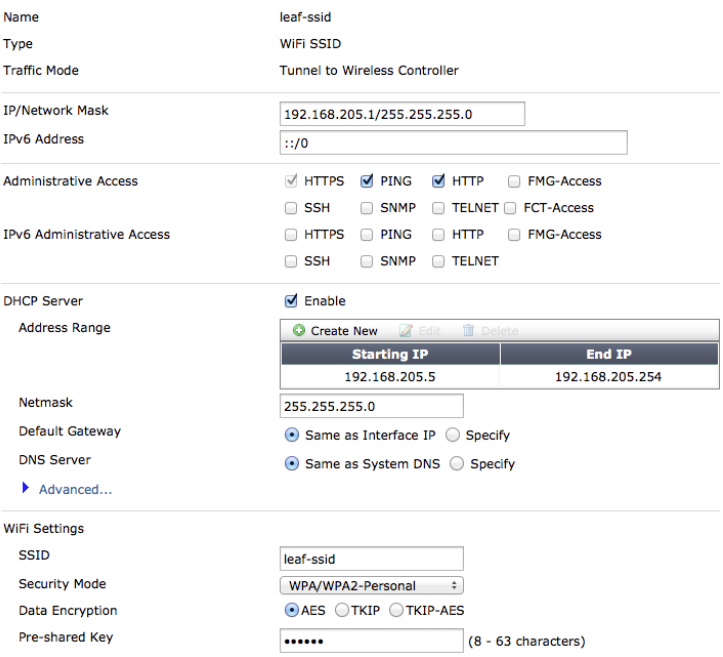
Go to **System > Network > Interfaces** and create the backhaul SSID.

Set **Type** to **WiFi SSID** and configure the **WiFi Settings** as needed.



Create the leaf SSID.

Set **Type** to **WiFi SSID**, enable **DHCP Server**, and configure the **WiFi Settings** as needed.



Creating a custom AP profile

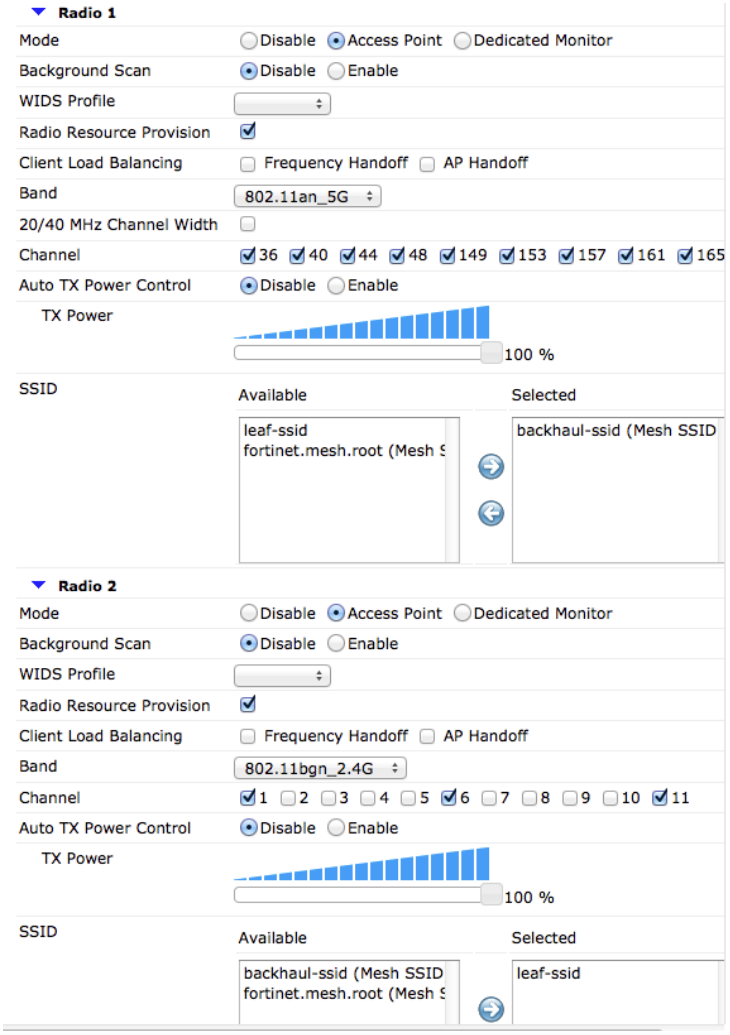
Go to **WiFi & Switch Controller > WiFi Network > Custom AP Profile**.

Create a new profile for the FortiAP model you are using.

Configure **Radio 1** for the backhaul channel and **Radio 2** for the leaf channel.

For the backhaul channel, set **Band** to **802.11an_5G**. For the leaf channel, set **Band** to **802.11bgn_2.4G**.

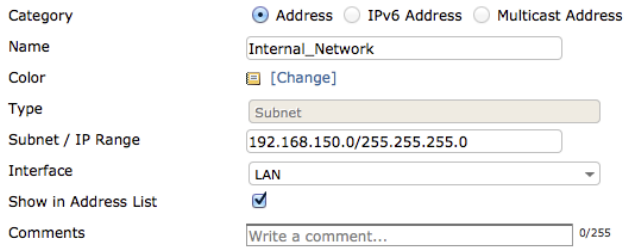
You may have to configure two custom AP profiles if your FortiAP units are different models that cannot use the same profile.



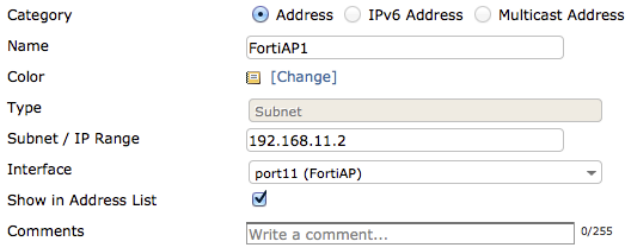
Creating firewall addresses and an address group

Go to **Firewall Objects > Address > Addresses**.

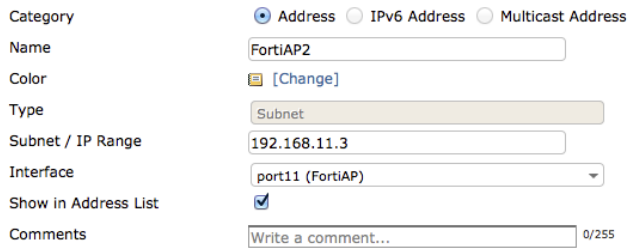
Create a new address for the internal network.



Create an address for FortiAP-1.



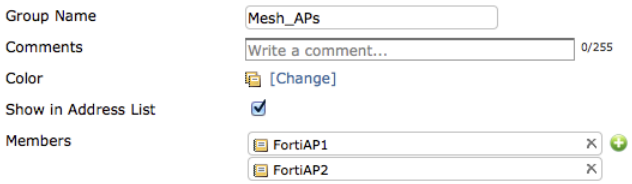
Create an address for FortiAP-2.



Create an address for leaf channel users, using the DHCP range used by the leaf channel SSID.

Go to **Firewall > Address > Groups** and create a new group.

Add the FortiAP addresses to the group.



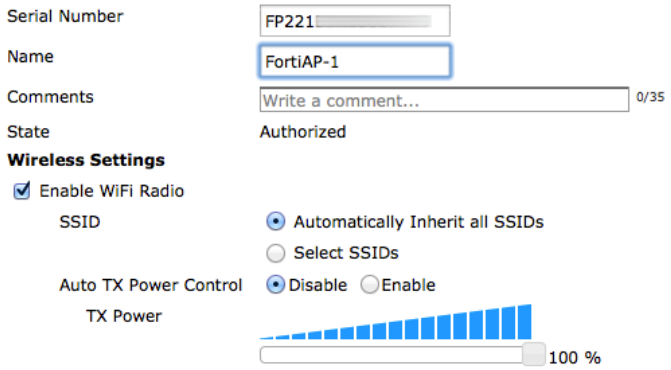
Setting up and configuring the FortiAPs

In this example, the FortiAP-221B unit is FortiAP-1, while the FortiAP-220B is FortiAP-2.

Preauthorize FortiAP-1

Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAP**. Select **Create New.**

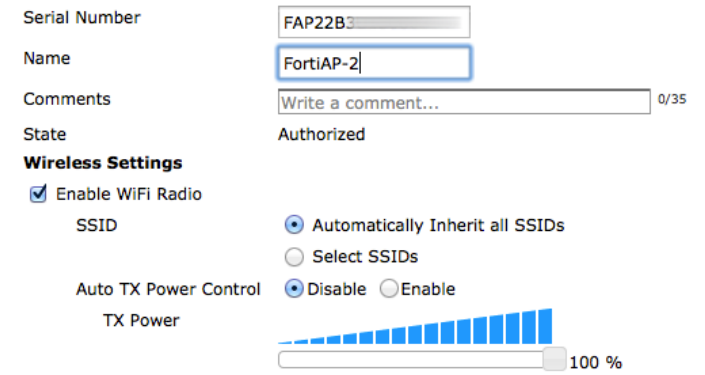
Enter the serial number of the FortiAP unit and give the Managed Access Point a name.



Preauthorize FortiAP-2

Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAP**. Select **Create New**.

Enter the serial number of the FortiAP and give the Managed Access Point a name.



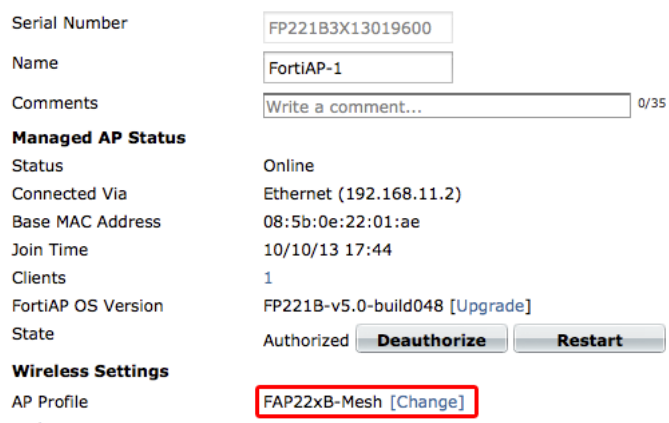
The FortiAP list will now show both FortiAP units. Since they are not currently connected, they will appear greyed out.

Apply the Custom AP profile

Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAP.**

The same custom AP profile needs to be added to both the FortiAP units. Edit each one in turn.

Use the **[Change]** link to assign the custom AP profile.



The FortiAP list now shows that the SSIDs have been added to the appropriate radios on the APs.

Access Point	State	Connected Via	SSIDs
FortiAP-1		-	Radio 1: backhaul-ssid Radio 2: leaf-ssid
FortiAP-2		-	Radio 1: backhaul-ssid Radio 2: leaf-ssid

Configure FortiAP-1 through its web interface

Certain parameters of the FortiAP units can only be configured by connecting to the unit directly, rather than through the FortiGate interface.

Reset the IP information of your computer to an address on the same subnet as the FortiAP. If the AP is in its factory default configuration, use the following address:

IP address:	192.168.1.100
Subnet mask:	255.255.255.0
Gateway:	192.168.1.1

Connect your computer to the FortiAP with an Ethernet cable. One end of the Ethernet cable connected to the network interface port of you computer and the other connected to the POE interface on the AP.

Open a browser window and use the IP address of the FortiAP unit as the URL. The factory default IP address is *192.168.1.2.* Login with the name: *admin*. Password is null, so just press Login.

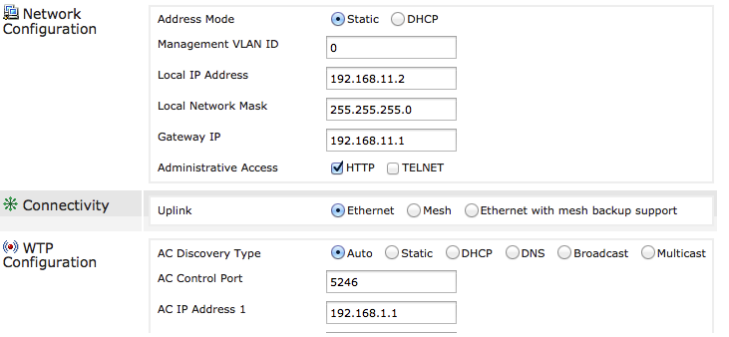
If this does not work, use the reset button to return the FortiAP to default settings.

Set **Address Mode** to **Static** and set **Local IP Address** to the same address as previously set on the FortiGate unit.

Set **Uplink** to **Ethernet** and **AC Discovery Type** to **Auto.**

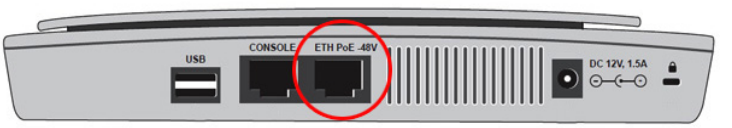
Once the changes have been made, you will not be able to connect to the FortiAP unit through the web interface, because it is no longer on the same subnet as your computer.

Do not reset the IP configuration on the computer yet as you still need to configure FortiAP #2 and the same addresses will be used on both sides of the Ethernet connection.



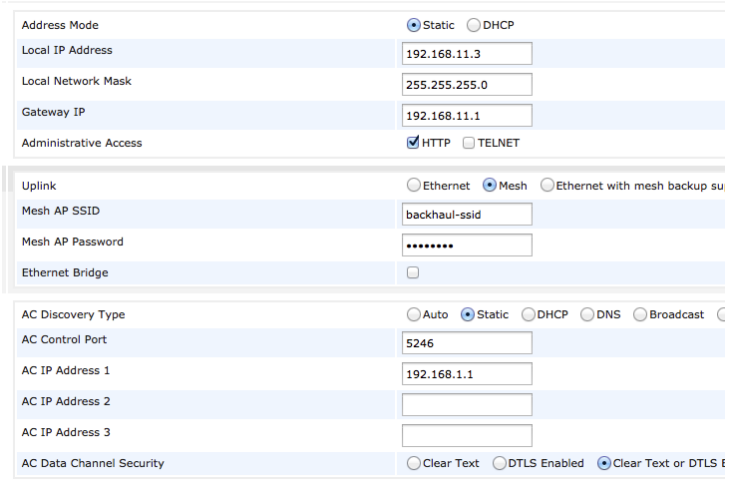
Configure AP-2 through its web interface

As with the AP-1, connect to the web interface. Make sure to use the correct Ethernet porte.



Set **Address Mode** to **Static** and set **Local IP Address** to the same address as previously set on the FortiGate unit.

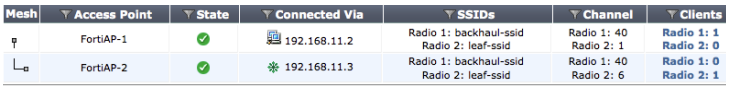
Set **Uplink** is set to **Mesh**, the **AC Discover Type** to **Static**, and **AC IP Address 1** to the IP interface of the FortiGate port that is dedicated to the FortiAPs.



Reset the computer to its normal IP address configuration and login to the FortiGate unit.

Connect FortiAP-1 to the FortiGate interface dedicated to the FortiAPs (in the example, port 11).

Once the FortiAPs are configured and powered up, they should no longer be shown as online. The **Mesh** column will also show that FortiAP-2 is connected through a mesh to FortiAP-1.



(Alternative) Configure AP-2 through its console port

FortiAP-2 in the example is a FAP-220B. This model includes a console port. This allows for the option of using the CLI to configure the unit.

Instead of an Ethernet cable, use a console cable to connect from your computer to the console port of FortiAP #2. The exact details of connecting will defer slightly based on whether the console cable is connected directly from a serial port or through a USB adapter and what operating system is on your computer, but once the connection has been made it proceeds as follows:

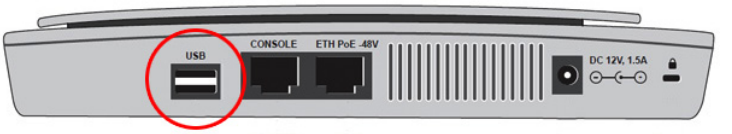
Using a utility like Putty or Terminal, connect to the CLI. For more details on connecting read the Quick Start Guide for the model.

Login with the credentials:

Username: admin

Password: <null>

Use the following commands to change the network configuration.



Change Address Mode to Static:

```
cfg -a ADDR_MODE=STATIC
cfg -c
```

Set the IP address:

```
cfg -a IPADDR=192.168.11.3
cfg -a AP_NETMASK:=255.255.255.0
cfg -a IPGW=192.168.11.1
cfg -c
```

Change Connectivity, remebering to choose a more secure password:

```
cfg -a MESH_AP_TYPE:=1
cfg -a MESH_AP_SSID:=backhaul-ssid
cfg -a MESH_AP_PASSWD:=12345678
cfg -c
```

Assign the discovery type to Static:

```
cfg -a AC_DISCOVERY_TYPE=1

cfg -c
```

Statically assign the IP address for the Access Controller (AC):

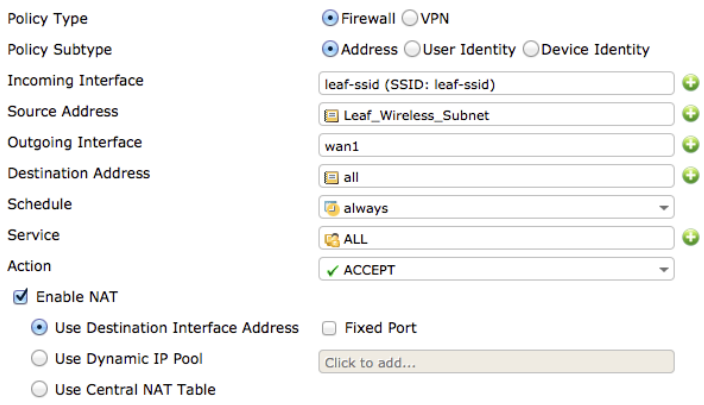
```
cfg -a AC_IPADDR=192.168.11.1

cfg -c
```

Creating security policies on the FortiGate

Go to **Policy > Policy > Policy** and create a policy to allow wireless users out to Internet

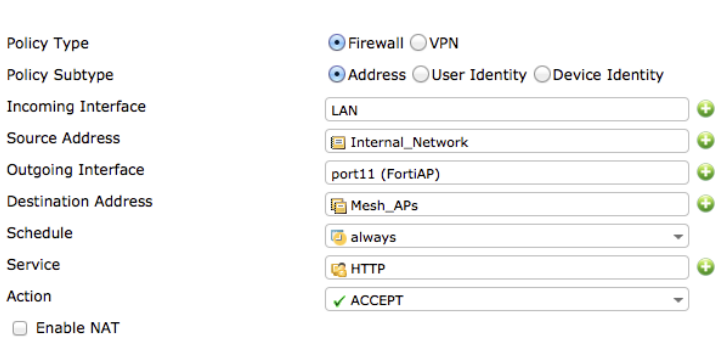
Set **Incoming Interface** to the leaf SSID, **Source Address** to the address for leaf channel users, **Outgoing Interface** to your Internet-facing interface, and **Enable NAT**.



Create another policy to allow traffic to reach APs. This is primarily to allow access to the web interfaces of the FortiAPs, so if you wish you can limit the policy to only allow access to those IP addresses.

Set **Incoming Interface** to the internal network's interface (in the example, **LAN**), **Source Address** to the address for the internal network, **Outgoing Interface** to the port dedicated to the FortiAPs, and (optionally) **Destination Address** to the group containing both FortiAP addresses.

After policies are created, remember to place them at a proper point in the sequence so that they can be reached by the desired traffic but will not interfere with other traffic.



Results

Wireless devices are now able to connect to the leaf SSID, even if they are only within the range of FortiAP-2.

There are several ways to verify that the wireless network has been extended over both FortiAP units.

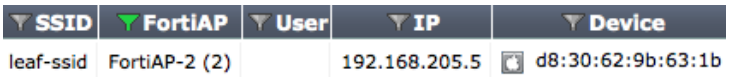
Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAPs**.

You can see that **Radio 2** (leaf-ssid) on FortiAP-2 has one client connected to it, while the same SSID on FortiAP-1 does not.

SSIDs	Channel	Clients
Radio 1: backhaul-ssid Radio 2: leaf-ssid	Radio 1: 40 Radio 2: 1	Radio 1: 1 Radio 2: 0
Radio 1: backhaul-ssid Radio 2: leaf-ssid	Radio 1: 40 Radio 2: 6	Radio 1: 0 Radio 2: 1

Go to **WiFi & Switch Controller > Monitor > Client Monitor**.

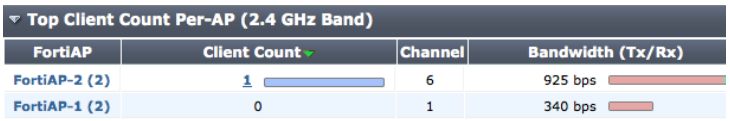
The client monitor which SSID and FortiAP that a client is connected to. In the example, a client has successfully connected to the leaf SSID on FortiAP-2.



SSID	FortiAP	User	IP	Device
leaf-ssid	FortiAP-2 (2)		192.168.205.5	d8:30:62:9b:63:1b

Go to **WiFi & Switch Controller > Monitor > Wireless Health**.

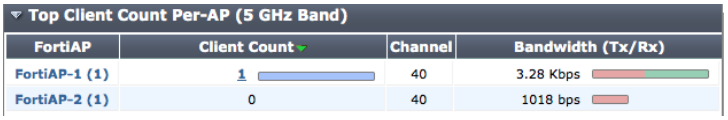
For information on the leaf channel, which uses the 2.4 GHz frequency, view the **Top Client Count Per-AP (2.4 GHz Band)** widget. In the example, the only SSID on that frequency is for the leaf channel, so the client using radio 1 on FortiAP-2 must be using that SSID.



Top Client Count Per-AP (2.4 GHz Band)

FortiAP	Client Count	Channel	Bandwidth (Tx/Rx)
FortiAP-2 (2)	1	6	925 bps
FortiAP-1 (2)	0	1	340 bps

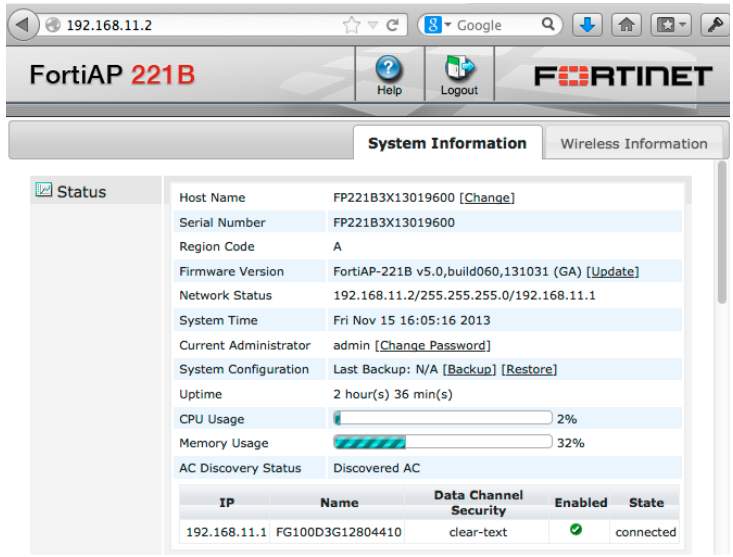
For information on the backhaul channel, which uses the 2.4 GHz frequency, view the **Top Client Count Per-AP (5 GHz Band)**. Again, in the example configuration, the only SSID on this frequency is for the backhaul channel.



Top Client Count Per-AP (5 GHz Band)

FortiAP	Client Count	Channel	Bandwidth (Tx/Rx)
FortiAP-1 (1)	1	40	3.28 Kbps
FortiAP-2 (1)	0	40	1018 bps

Open a browser and verify that you can connect to the web interface of FortiAP-1, using the IP set in the configuration (in the example, *http://192.168.11.2*).



Connect to the web interface of FortiAP-2 using its assigned IP (in the example, *http://192.168.11.3*).